IN THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA,	)	
	)	
v.	)	Case No. 1:23CR65-CMH
	)	
JAMES MEEK.	)	

MOTION TO SUPPRESS THE EVIDENCE OBTAINED AS A RESULT OF THE WARRANTLESS SEARCH OF MR. MEEK'S DROPBOX ACCOUNT AND THE CONTENTS THEREOF

James Gordon Meek, through counsel, and pursuant to Rule 12(b)(3) of the Federal Rules of Criminal Procedure and the Fourth Amendment to the United States Constitution, respectfully moves the Court to suppress the evidence obtained as a result of the warrantless search of the Dropbox account associated with [redacted] as well as the contents of that account. All of the evidence in this case stems from this illegal search and seizure, and should be suppressed.[1] In support of his motion, Mr. Meek states as follows:

BACKGROUND

Mr. Meek is charged by indictment with three counts: (1) transportation of child pornography in violation of 18 U.S.C. §§ 2252(a)(1) and (b)(1); (2) distribution of child pornography in violation of §§ 2252(a)(2) and (b)(2), and (3) possession of child pornography in violation of §§ 2252(a)(4)(B) and (b)(2). ECF 39—Indictment.

[1] Given that the government has not disclosed all discovery to the defense, defense investigation of this case is incomplete at this stage. *See generally* Motion to Compel, ECF 46. Mr. Meek therefore reserves the right to move for suppression of evidence based on grounds not now discernible such as, but not limited to, rights under *Franks v. Delaware*, 438 U.S. 154 (1978).

On March 11, 2021, Dropbox, Inc. ("Dropbox") sent a CyberTip to the National Center for Missing and Exploited Children ("NCMEC") containing five video files it had "found" constituting child sexual abuse material ("CSAM"). The government's affidavit in support of the search of Mr. Meek's residence states as follows: "The investigation was initiated from an investigative lead sent to the Washington Field Office's Child Exploitation and Human Trafficking Task Force. The lead stated that on March 11, 2021, Dropbox filed a CyberTip with the National Center for Missing and Exploited Children (NCMEC) regarding child pornography found in a Dropbox account on March 10, 2021. The CyberTip reported that a Dropbox account user had uploaded five videos to Dropbox that were later confirmed by law enforcement to contain child pornography. The username associated with the account was "James Meek," and the CyberTip contained IP addresses that were subsequently determined to be assigned to MEEK, at an address in Arlington, VA (MEEK's RESIDENCE)." Exhibit 1—Redacted Affidavit in Support of Search Warrant for Residence and Devices, ¶ 7.

Dropbox also sent a "metadata" file that reflects the dates that the five videos at issue were uploaded to Dropbox, or moved among folders on the Dropbox account. Exhibit 2—Metadata file. The earliest date on the metadata file indicates that a video was added on August 8, 2018, while the latest date indicates that a video was added on December 30, 2020. *Id.* The Dropbox account at issue was linked to the email address [redacted]

NCMEC generated a report relating to this CyberTip. Exhibit 3—NCMEC Report. The NCMEC CyberTip report reflects that the five video files were "found" by Dropbox on March 10, 2021, but also states that date may have been generated by default based on the date of the CyberTip itself. *Id.* at 1 ("Incident Information"). The report states that three of the five videos sent with the tip matched the hash values for known CSAM videos, while two did not. *Id.* at 4-5.

The report states that NCMEC reviewed the two videos that did not match the hash values of previously identified CSAM files. *Id.* at 6. For each of the five videos, NCMEC's report has entries that state as follows: "Did reporting ESP view entire contents of uploaded file? Yes." *Id.* at 2-3. The defense has received no documents or information from Dropbox relating to its actions in connection with the discovery, identification or examination of the files at issue. The government has not responded to the defense requests for this information.

NCMEC forwarded the CyberTip to the Virginia State Police on April 5, 2021. *Id.* at 8. The Virginia State Police then investigated the case by issuing subpoenas to Verizon and Google. At some unknown point, and for unknown reasons, the case was referred to Arlington County Police Department. It is not clear what investigation the Arlington County Police conducted before they allegedly referred this matter to the FBI in September of 2021.

At some point, at least two FBI agents watched the entirety of the five videos reported to NCMEC, and did so without a warrant. *See, e.g.*, Ex 1 at ¶ 17 (Agent Laura Calvillo's Affidavit).[2] The agents relied on the Dropbox CyberTip and the content of the videos to obtain multiple search warrants:

- A search warrant for the Dropbox account associated with [redacted] issued on November 10, 2021;
- A search warrant to search Mr. Meek's residence and seize a wide variety of items therein, including digital devices, issued April 22, 2022.

The evidence seized in the search of the residence on April 27, 2022, in combination with the prior Dropbox search, was the basis for subsequent warrants:

- A search warrant for the Snapchat account issued November 14, 2022;

[2] The affidavit in support of the November 10, 2021 search warrant was prepared by Agent Richard Guida, who also attested that he watched the five videos reported by Dropbox to NCMEC.

- A search warrant for the Apple accounts associated with the email addresses [redacted] issued November 14, 2022.

For the reasons that follow, all of the warrants in the case, which rely entirely on Dropbox's alleged discovery of the videos and the government's subsequent warrantless review of those videos, should be suppressed.

ARGUMENT

I. APPLICABLE LAW.

A warrantless seizure is "*per se* unreasonable . . . subject to only a few specifically established and well-delineated exceptions." *Katz v. United States,* 389 U.S. 347, 357 (1967). Courts have previously held that when a search is conducted purely by a private party, it does not constitute a search within the scope of the Fourth Amendment. *See, e.g., United States v. Jacobsen*, 466 U.S. 109 (1984). However, the private party search doctrine does not apply if law enforcement agents were involved in the search. *See, e.g., Skinner v. Ry. Labor Executives' Ass'n*, 489 U.S. 602 (1989) (holding that a private party's search is attributable to the government "if the private party acted as an instrument or agent of the Government."); *United States v. Hardin*, 539 F.3d 404, 419 (6th Cir. 2008) (finding a search illegal where the police "instigated, encouraged or participated in the search" and the private citizen "engaged in the search with the intent of assisting the police in their investigative efforts."); *Cf. United States v. Richardson*, 607 F.3d 357, 366 (4th Cir. 2010) (holding that AOL's scanning of email communications for child pornography and reporting discoveries to NCMEC did not trigger the Fourth Amendment's warrant requirement because no law enforcement officer or agency asked the provider to conduct the search).

Furthermore, even if the initial search was conducted purely by a third party, a subsequent search by the government that exceeds the scope of the initial search by the private party constitutes an illegal search, in violation of the Fourth Amendment. *See, e.g., Walter v. United States,* 447 U.S. 649. 556-60 (1980) (holding that while a private party read the labels indicating a misdelivered pornographic film was obscene, and held up and viewed the film stock that it later turned over to law enforcement, law enforcement's subsequent viewing of the film by projecting it onto a screen without a warrant exceeded the scope of the private party's search and therefore rendered it an unlawful search in violation of the Fourth Amendment); *United States v. Wilson*, 13 F.4th 961 (9th Cir. 2021) (finding that law enforcement exceeded the scope of a private search by Google when opening emails and files that a Google employee did not previously view); *United States v. Ackerman*, 831 F.3d 1292, 1294 (10th Cir. 2016) (Gorsuch, J.) (holding that NCMEC was a government actor or agent of the government that conducted a warrantless search by reviewing email attachments that were reported but not previously opened by AOL); *United States v. Sparks*, 806 F.3d 1323 (11th Cir. 2015) (finding that a police officer's warrantless review of a video on a cell phone that had not been reviewed by a private party was a Fourth Amendment violation) *overruled on other grounds, United States v. Ross*, 963 F.3d 1056 (11th Cir. 2020); *United States v. Lichtenberger*, 786 F.3d 478 (6th Cir. 2015) (police search of contents of defendant's computer exceeded the scope of the prior search by his girlfriend, and therefore violated the Fourth Amendment).

The government bears the burden to prove both that the private party search exception to the warrant requirement applies here, and that the scope of the government's search did not exceed the scope of the private search. In *Coolidge v. New Hampshire*, the Supreme Court stressed that

> the most basic constitutional rule in this area is that searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well delineated exceptions. The exceptions are 'jealously and carefully drawn . . . The burden is on those seeking the exemption to show the need for it.

403 U.S. 443, 454–55 (1971) (internal citations, quotation marks and footnotes omitted). *See also Nix v. Williams,* 467 U.S. 431, 444 (1984) (noting that "the cases implementing the exclusionary rule 'begin with the premise that the challenged evidence is in some sense the product of illegal governmental activity'" and that the government bears the burden to show that the search at issue was lawful (quoting *United States v. Crews*, 445 U.S. 463, 471 (1980)); *United States v. Mendenhall,* 446 U.S. 544, 557 (1980) (government had the burden to prove that the defendant's confession was not the result of coercion); *United States v. Johnson*, 14 F.3d 597 n.7 (4th Cir. 1994) ("Because an inventory search is an exception to the warrant requirement, the burden is on the government to demonstrate that the inventory search was permissible.").

For the reasons discussed below, the third party search exception does not apply because law enforcement agents were involved in Dropbox's search of the contents of the account. Alternatively, even if the private search exception could apply, the government exceeded the scope of the private search.

II. THE DROPBOX ACCOUNT AND THE FIVE VIDEOS WERE SEIZED AND SEARCHED IN VIOLATION OF THE FOURTH AMENDMENT.

A. The Government Conducted a Warrantless Search in Violation of Mr. Meek's Legitimate Expectation of Privacy in his Dropbox Account.

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. Amend. IV. The Fourth Amendment's protections apply when there is a "search" within the meaning of the Fourth Amendment when the government intrudes or trespasses upon a constitutionally protected area, including "persons, houses, papers, [or] effects" . . . "for the purpose of obtaining

information." *United States v. Jones*, 565 U.S. 400, 404 (2012). In addition, a Fourth Amendment "search" occurs when a government agent infringes on "an expectation of privacy that society is prepared to consider reasonable[.]" *Jacobsen*, 466 U.S. at 113; *see also Jones*, 565 U.S. at 409 (the "reasonable-expectation-of-privacy test has been added to, not substituted for, the common-law trespassory test.").

Mr. Meek has standing to contest the search and seizure warrants. *Rakas v. Illinois*, 439 U.S. 128 (1978). Mr. Meek had a legitimate expectation of privacy in the contents of his Dropbox account which stores digital documents belonging to its owner, similar to an email account or the contents of a cell phone or computer. *See, e.g., Riley v. California*, 573 U.S. 373, 397 (2014) (recognizing legitimate privacy interests in the contents of a cell phone, which are often also stored in the cloud); *Carpenter v. United States*, 138 S. Ct. 2206, 2219 (2018) (finding that individuals have a privacy interest in the location data generated by their cell phone); *United States v. Warshak*, 631 F.3d 266, 283–88 (6th Cir. 2010) (finding Fourth Amendment protection for email contents). A password-protected Dropbox account is the modern digital equivalent of a traditional filing cabinet or safe located within a private home. The government cannot break into such things without a warrant, or instigate such a break-in by a private party. Such acts violate the Fourth Amendment.

Mr. Meek also had a Fourth Amendment property interest in the Dropbox account and its contents. See, e.g., *Ex Parte Jackson*, 96 U.S. 727, 733 (1877) ("[l]etters and sealed packages . . . in the mail are as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles . . . [t]he constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection,

wherever they may be. Whilst in the mail, they can only be opened and examined under like warrant, issued upon similar oath or affirmation, particularly describing the thing to be seized, as is required when papers are subjected to search in one's own household."); *Carpenter*, 138 S. Ct. at 2269 (Gorsuch, J. dissenting) ("few doubt that e-mail should be treated much like the traditional mail it has largely supplanted—as a bailment in which the owner retains a vital and protected legal interest."); *United States v. Kernell*, 2010 U.S. Dist. LEXIS 36477, *13-15 (E.D. Tenn. 2010) (an individual has a property right to the exclusive use of the information and pictures contained in her email account).

Accordingly, the Court should suppress all of the evidence obtained pursuant to the search warrants in this case as the result of a warrantless search of the Dropbox account and the five specific files contained therein.

B. The Private Search Exception Does Not Apply.

The private party search exception does not apply in this case. First, as a general matter, there is a substantial question as to whether the third party search exception has any viability in the context of a search of an online account such as Dropbox, given the Supreme Court's recent decisions. In *Riley v. California*, 573 U.S. 373, 397 (2014), the Court declined to extend the search-incident-to-arrest exception to cell phones. Then, in *Carpenter*, the Court refused to extend the third party search doctrine to cell phone location records generated by cell phone providers. *Carpenter v. United States*, 138 S. Ct. 2206, 2219 (2018) "The third-party doctrine partly stems from the notion that an individual has a reduced expectation of privacy in information knowingly shared with another. But the fact of "diminished privacy interests does not mean that the Fourth Amendment falls out of the picture entirely." *Id.* *See also United States v. Jones*, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) (explaining that the third-party

doctrine "is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks"). Given this recent case law, Mr. Meek respectfully submits that the third party search doctrine no longer provides an exception to warrantless searches by entities such as Dropbox, whose entire existence rests on providing a private and secure site of online electronic storage of private information, fully the equivalent of papers locked up inside a private home, which plainly was at the core of the Fourth Amendment's protections as intended by the Framers

C. Assuming the Private Search Exception Can Apply in this Context, the Search of Dropbox Was Not a Private Search.

Assuming *arguendo* that the private search exception applies generally, it does not apply in this case. The facts in this case show that law enforcement was involved in the warrantless search of Mr. Meek's Dropbox account. While we do not know what Dropbox actually did with the five files, it is clear that the FBI already knew about the CSAM videos in the Dropbox account before they were ever reported to NCMEC. We know this because the FBI sent a preservation letter pursuant to 18 U.S.C. § 2703(f) on that very same day to Google for [redacted], the email account linked to the Dropbox account in which the CSAM was "discovered." Ex. 4—March 10, 2021 preservation letter to Google relating to the [redacted] account.[3] How could the FBI draft and send a letter to Google before it had received the CyberTip supposedly sent by Dropbox to NCMEC?

Furthermore, while the last instance of activity involving any of the alleged CSAM files occurred in December of 2020, these files were not "found" until more than three months later. This indicates that the files were not located as the result of a routine process. In sum, the

[3] The agent sending the letter is a Supervisory Special Agent in the FBI's Child Exploitation Section.

evidence in this case shows that law enforcement was involved in Dropbox's warrantless search and seizure of the five files as issue. Under these circumstances, the private search exception does not apply because Dropbox "acted as an instrument or agent of the Government." *Skinner*, 489 U.S. 602 (1989). *See also Hardin*, 539 F.3d at 419.

D. The Government's Review of the Five Video Files at Issue Without a Warrant Exceeded the Scope of Any Private Search.

Even assuming *arguendo* that no law enforcement officer was involved in Dropbox's search of Mr. Meek's account and the five CSAM files reported to NCMEC, the third party search exception would apply only if the scope of the government's review of the five files—which involved playing and viewing each video—was no broader than the scope of Dropbox's initial review of the files. The government bears the burden of proof to show this fact. *Wilson*, 13 F.4th at 971 ("The government bears the burden to prove [the] warrantless search was justified by the private search exception to the Fourth Amendment's warrant requirement.").

But the government has not provided any information regarding what Dropbox actually did in its examination of the files, and the NCMEC report fails to fill this void. For starters, the report is not created by the individual at Dropbox who conducted the review, and thus has personal knowledge of exactly what was done; it is created by an agent of the government (NCMEC) with no knowledge of what actually happened. Furthermore, the language of the NCMEC report is unclear as to what is meant by "view[ing] entire contents of uploaded file." In *Walter*, for example, the private party "viewed" the film by holding the film stock up to the light, but this differed from law enforcement's viewing of the film by screening it. In this case, the Court must determine precisely what Dropbox did in its examination of the videos reported to NCMEC before it can determine whether the government's warrantless review of those materials violated the Fourth Amendment. Unless and until the government comes forward with evidence

proving that the government search did not exceed the private search, the search must be presumed illegal.

E. The Private Search Exception is Not a Defense to the Violation of Mr. Meek's Property Interests in the Contents of the Dropbox Account.

Even if there was a private search in this case, and even if it overlapped perfectly with the government's subsequent warrantless search, the private search doctrine does not provide the government with a defense here because the government's actions also violated Mr. Meek's property interests in the contents of the Dropbox account.

The entire premise behind the third party search exception is that a third party's private search already frustrated the defendant's privacy interests, and a government search of the same material does not further frustrate the privacy interest. *See, e.g, Walter*, 447 U.S at 659. But courts have recognized that in the Fourth Amendment context, property interests are distinct from privacy interests. *See, e.g., Carpenter*, 138 S. Ct. at 2223 (holding that despite the fact that Carpenter's location data was held by the cell phone carrier, it was nevertheless protected from warrantless government intrusion); *see also Carpenter*, 138 S. Ct. at 2270 (Gorsuch, J. dissenting) ("just because you *have* to entrust a third party with your data doesn't necessarily mean you should lose all Fourth Amendment protections in it") (emphasis in original); *Ackerman*, 831 F.3d at 1307 (explaining an individual who entrusts his property or data to a third party does not thereby forfeit his property rights, and explaining that a search that does not trigger a privacy interest may nevertheless violate an individual's Fourth Amendment property right) (citing *United States v. Jones*, —— U.S. ——, 132 S.Ct. 945 (2012)).

In this case, the government reviewed the videos from Mr. Meek's Dropbox account after the videos were sent to NCMEC, and NCMEC—recognized in Ackerman and other cases to be an arm or agent of the government—in turn created another copy of the videos and sent them to

the Virginia State Police. The Virginia State Police then created at least one further copy of the materials and sent them to the Arlington County Police Department and/or the FBI. All of these actions violated Mr. Meek's property interests in the videos. *See United States v. Bach*, 310 F.3d 1063, 1067-68 (8th Cir. 2002) (analyzing the copying and review of stored Internet contents held by an Internet provider as a Fourth Amendment "seizure" and a "search" of the contents); *Vaugh v. Baldwin*, 950 F.2d 331, 334 (6th Cir. 1991) (noting that, in the absence of consent, the government had "no right to . . . photocopy" a person's private documents); *United States v. Loera*, 333 F. Supp. 3d 172, 185 (E.D.N.Y. 2018) ("Most courts that have addressed duplication, including digital duplication, have analyzed it as a seizure."); Fed. R. Crim. Pro. 41(e)(2)(B) (equating the seizure of electronically stored information with the copying of the information).

For all of these reasons, even if the government can meet its burden that the private search exception applies in this case to the privacy rights in the Dropbox account, this exception does not apply to the government's violation of Mr. Meek's property interests in the account and its contents.

III. THE EVIDENCE SEIZED PURSUANT TO THE WARRANTS IN THIS CASE MUST BE SUPPRESSED.

Without the illegally seized videos, there was insufficient probable cause in this case to authorize the search and seizure warrants. *See Doe v. Broderick*, 225 F.3d 440, 451 (4th Cir. 2000). Therefore, all evidence and information obtained as a result of the invalid warrants, as well as all derivative evidence and statements, should be suppressed. *See generally Weeks v. United States*, 232 U.S. 383 (1914) (establishing the exclusionary rule that bars the use of illegally obtained evidence at trial); *Wong Sun v. United States*, 371 U.S. 471 (1963).

CONCLUSION

For all the foregoing reasons, the Court should suppress all of the evidence obtained as a result of the warrantless search of Mr. Meek's Dropbox account, and the contents thereof.

Respectfully Submitted,

By: /s/ *Eugene V. Gorokhov*
Eugene Gorokhov, Bar No. 73582
Attorney for Defendant
BURNHAM & GOROKHOV, PLLC
1750 K Street NW, Suite 300
Washington, DC 20006
(202) 386-6920 (phone)
(202) 765-2173 (fax)
eugene@burnhamgorokhov.com

CERTIFICATE OF SERVICE

I hereby certify that I filed the foregoing document VIA ECF which provides a copy to the AUSA of record.

By: /s/ *Eugene V. Gorokhov*
Eugene Gorokhov, Bar. No. 73582
Attorney for Defendant
BURNHAM & GOROKHOV, PLLC
1750 K Street NW, Suite 300
Washington, DC 20006
(202) 386-6920 (phone)
(202) 765-2173 (fax)
eugene@burnhamgorokhov.com